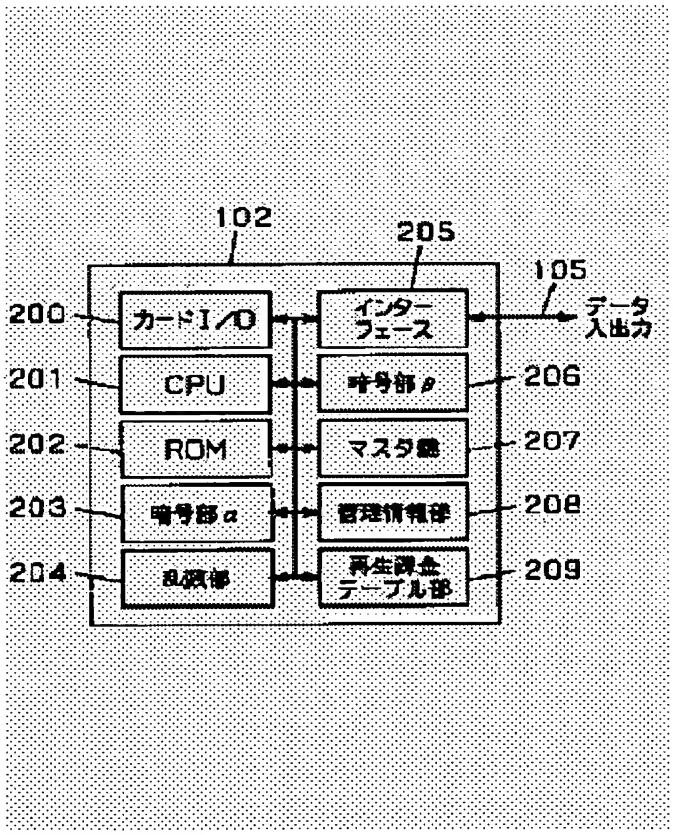
DATA MANAGEMENT CARD

Publication number: JP2001077806
Publication date: 2001-03-23
Inventor: KASHIWA HIROSHI
Applicant: MATSUSHITA ELECTRIC IND CO LTD
Classification:
- international: ***G06K19/00; G06F15/00; G06F21/00; H04L9/14; H04L9/32; H04N7/16;*** **G06K19/00; G06F15/00; G06F21/00; H04L9/14; H04L9/32; H04N7/16;** (IPC1-7): H04L9/14; G06F15/00; H04L9/32; H04N7/16
- European:
Application number: JP19990248350 19990902
Priority number(s): JP19990248350 19990902

Abstract of **JP2001077806**

PROBLEM TO BE SOLVED: To ensure a copyright protection function of contents recorded in a medium and to secure security required for it by using a card provided with an interface. SOLUTION: A card 102 has different encryption algorithm sets (encryption sections &alpha , &beta), the encryption section &alpha 203 decodes contents that are encrypted and transmitted, the encryption section &beta 206 is used at recording, the contents that are encrypted by using a random number for a key and an identification code using the random number are recorded in a medium, the card has the identification code by each title of the contents and the decoding key, the identification code is used at reproduction of contents, key information not open to public is decoded at an outside of the card so as to attain copyright management such as output of contents to other recorder without recording the copyright protection information like the decoding key to the medium.



[0033]

(Recoding content on media)

The following will explain an operation for recording contents from a broadcast source station 100 to a reception, recording and reproducing apparatus 101. FIG. 4 shows a configuration view of a card 102.

[0034]

In FIG. 4, 200 denotes a card I/O for performing data transmission and reception with the reception, recording and reproducing apparatus 101, 201 denotes a CPU that controls the card 102, 202 denotes a ROM that stores a program executed by the CPU 201, 203 is an encryption section α having cryptographic algorithm for use in content to be distributed from the broadcast source station 100, 204 denotes a random number generator, 205 denotes an interface that performs data transmission and reception with an outer device of the reception, recording and reproducing apparatus 101, 206 denotes an encryption section β having cryptographic algorithm for use in recording distributed content on media and the like, 207 denotes a master key that is a key for decoding encrypted content distributed from the broadcast source station, 208 denotes a management information section that is configured by an involatile memory that stores information necessary for reproducing content, and 209 denotes a reproduction charging table section that is configured by an involatile memory to be used in processing reproduction charging to be described later.

[0035]

FIG. 5 is a configuration view of the reception, recording and reproducing apparatus 101. In FIG. 5, 210 denotes a network interface for performing data transmission and reception with the broadcast source station 100 through a public network 103, 211 denotes an expansion processing section that decodes data of MPEG video and audio, 212 denotes a card I/O for performing data transmission and reception with card 102, 213 denotes a signal processing section that creates a recording format, 214 denotes a laser drive section, 215 denotes an optical head section, 216 denotes a disk, 217 denotes a CPU that controls the reception, recording and reproducing apparatus 101, and 218 denotes a setting section 218 that sets an operation of the reception, recording and reproducing apparatus 101 by a user.

[0036]

Here, the card 102 is installed in the reception apparatus 101 so as to allow communications using the card I/O 200 and the card I/O 211 of the reception, recording and reproducing apparatus 101.

[0037]

Table 1 shows a format of storage data in the management information section 208, 300 denotes a content title, 301 denotes an identification code for performing identification for each content, 302 denotes a key to be used when the content is encrypted and recorded, 303 denotes a copy number restriction code for restricting the number of times when the content is output to an outer section, 304 denotes a class code for identifying a rate for reproduction charge when recording on

the medium is performed for each content, 305 denotes a date code indicating date when recording is performed for each content, 306 denotes a reproduction restriction code for restricting quality of the content recorded on the medium when outputting it to the outer section of the reproduction apparatus, 307 denotes a trace code for recording a distribution source for each content when the content is recorded, and 308 denotes a charging rate when reproduction charging is carried out.

[0038]

[Table 1]

				REPRODUCTION CHARGING SECTION				
TITLE 300	IDENTIFICATION CODE 301	KEY 302	COPY NUMBER RESTRICTION CODE 303	CLASS CODE 304	DATE CODE 305	REPRODUCTION RESTRICTION CODE 306	TRACE CODE 307	CHARGING RATE 308
X	B	A	2	T1	1999.4	011		
.	.	.	.					
.	.	.	.					

[0039]

The following will explain an operation for recording a content of a title X to the reception, recording and reproducing apparatus 101. First, the content transmitted in an encrypted format from the broadcast source station 100 via the network 103 is received by the network interface 210 of the reception,

recording and reproducing apparatus 101 and is transmitted to the card 102 through the card I/O 212.

[0040]

In the card 102, a control program of the ROM 202 is executed by the CPU 201, whereby the random number generator 204 generates a first random number to serve as a key A in step S11 as shown in FIG. 6. In step S12, the random number generator 204 generates a second random number to serve as a random number A. In step S13, the random number A is compared with information registered as an identification code in the management information section 208. When a match is found (No), step S12 is executed, and when no match is found (Yes), the random number A is used as an identification code B in step S14. This creates a pair of identification codes that can distinguish between a key for encrypting content at a recording time to be described later and a key that is stored in the card 102 necessary for decoding the content at a reproducing time.

[0041]

Then, the content input through the card I/O 200 is decoded in a predetermined unit by the encryption α 203 using the master key 207, the content is encrypted by the encryption section β 206 using the key A, and the identification code B and the encrypted content are transmitted to the reception, recording and reproducing apparatus 101 from the card I/O 200. Furthermore, the key A, identification code B and information, which is specifically described later and which is included in the header information section 117, are stored in the management

information section 208 on a title basis as shown in table 1. If no setting is made here, zero is set and the explanation is given as follows.

[0042]

The reception, recording and reproducing apparatus 101 converts the identification code and the content received by the card I/O 212 to a recording format after an error correction code for correcting an error is added by the signal processing section 213, and processing for converting the recorded information from an electrical signal to an optical signal is carried out by the laser drive section 214, and the result is recorded on the disc 216 by the optical head section 215.

[0043]

The cryptographic algorithm for use in distributing the content via the network is made different from the cryptographic algorithm for use in the media recordable or reproducible device by the aforementioned operation, whereby even if the cryptographic algorithm for use in the network is decoded, it is impossible to decode the content, which has been encrypted and recorded on the media, and this strengthen the safety of content copyright protection.

[0044]

Moreover, by converting the encryption of content in the card, it is possible to perform conversion of encryption as the security of content is maintained without making a plaintext, which is in the process of being converted, open to the public.

[Brief Description of the Drawings]

[FIG. 1] A configuration view of a transmission system according to one embodiment of the present invention;

[FIG. 2] A block diagram showing a content encryption transmission configuration in the same transmission system;

[FIG. 3] A transmission format confirmation view of the same transmission system;

[FIG. 4] A configuration view of a card used in the same transmission system; and

[FIG. 5] A configuration view of a reception, recording and reproducing apparatus of the same transmission system.

[FIG. 1]

RECEIVING SIDE

PUBLIC

TRANSMITTING SIDE

100: BROADCAST SOURCE STATION

[FIG. 2]

RECEIVING SIDE

110: DECODING

111: MASTER KEY

112: CONTENT KEY

CONTENT

PUBLIC

TRANSMITTING SIDE

109: MASTER KEY

108: CONTENT KEY

107: ENCRYPTING

CONTENT

[FIG. 3]

113: PREAMBLE

114: TRANSMISSION DESTINATION ADDRESS

115: TRANSMISSION SOURCE ADDRESS

116: DATA SECTION

117: HEADER INFORMATION SECTION

118: DECODING KEY INFORMATION SECTION

119: CONTENT INFORMATION SECTION

[FIG. 4]

200: CARD I/O

203: ENCRYPTION SECTION A

204: RANDOM NUMBER SECTION

205: INTERFACE

206: ENCRYPTION SECTION B

207: MASTER KEY

208: MANAGEMENT INFORMATION SECTION

209: REPRODUCTION CHARGING TABLE SECTION

DATA INPUT/OUTPUT

[FIG. 5]

210: NETWORK INTERFACE

211: EXPANSION PROCESSING SECTION

212: CARD I/O

213: SIGNAL PROCESSING SECTION

218: SETTING SECTION

214: LASER DRIVE

DATA INPUT/OUTPUT

VIDEO OUTPUT

AUDIO OUTPUT

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－77806
（P2001－77806A）
(43)公開日　平成13年３月23日(2001.3.23)

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
H04L 9/14		H04L 9/00	641	5B035
G06F 15/00	330	G06F 15/00	330Z	5B085
G06K 19/00		H04N 7/16	Z	5C064
H04L 9/32		G06K 19/00	Q	5J104
H04N 7/16		H04L 9/00	673E	

審査請求　未請求　請求項の数９　ＯＬ　（全 11 頁）

(21)出願番号　特願平11－248350

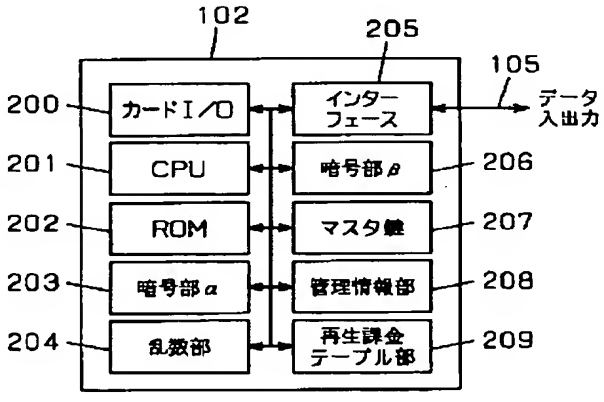
(22)出願日　平成11年９月２日(1999.9.2)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　柏　浩
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100097445
弁理士　岩橋　文雄　（外２名）

最終頁に続く

(54)【発明の名称】　データ管理カード

(57)【要約】
【課題】　インターフェースを備えたカードを用い、メディアに記録したコンテンツの著作権保護機能とそれに必要なセキュリティを確保する。
【解決手段】　異なる暗号アルゴリズム（暗号部α、β）をカード１０２に有し、暗号部α２０３で暗号化され伝送されてくるコンテンツを復号し、記録時は暗号部β２０６を用い、乱数を鍵として暗号化したコンテンツと乱数を用いた識別コードをメディアに記録し、カードにコンテンツのタイトル毎に識別コードと復号鍵を有し、コンテンツ再生時に識別コードを利用し、カード外部に鍵情報を未公開で復号化することで、復号鍵等の著作権保護情報をメディアに記録することなくコンテンツを他の記録装置への出力などの著作権管理をも可能とする。



1

【特許請求の範囲】

【請求項１】メディアへの記録または再生する機能を備えた装置と通信することでコンテンツの管理を行うための２種類以上の暗号アルゴリズムと、外部装置との通信を目的とするインターフェースを少なくとも有し、前記メディアに記録するデータに用いる暗号アルゴリズムと前記インターフェースで通信に用いる暗号アルゴリズムが異なることを特徴とするデータ管理カード。

【請求項２】乱数を発生する乱数発生器をさらに備え、前記メディアにコンテンツを暗号化して記録する場合、前記乱数発生器を用いて記録するコンテンツ単位（名）で暗号化するための鍵を作成し、記録するデータ単位（名）毎に異なる様に前記乱数発生器を用いて独特の識別コード情報を作成し、該カードと前記メディアに同一の識別コードを記憶することを特徴とする請求項１記載のデータ管理カード。

【請求項３】メディアに記録されているコンテンツのインターフェースから外部装置への出力を制限する複写回数制限コード情報を記憶し、前記複写回数制限コードを有するコンテンツを出力する場合にコンテンツ毎に複写回数制限コードを更新し所定値になることで外部への出力を不可能とすることを特徴とする請求項１記載のデータ管理カード。

【請求項４】メディアに記録したコンテンツを再生する毎に料金を徴収するための再生課金を行うために、コンテンツ毎に料金識別するための等級コードの情報と、日付を示す日付コードの情報と、前記日付コードにより前記等級コードを選択するための転送コードの情報を有し、前記ディスクへの記録時にコンテンツ毎に前記等級コードと前記日付コードを記憶し、再生時において前記等級コードより選択される料金を加算することを特徴とする請求項１記載のデータ管理カード。

【請求項５】メディアにインターフェースを介してコンテンツを記録する場合、該コンテンツの発信源を識別可能なトレースコードの情報を記憶することを特徴とする請求項１記載のデータ管理カード。

【請求項６】コンテンツの視聴の条件を制約する再生制約コードの情報を付加されたコンテンツをメディアに記録または再生する場合、記録時に再生制約コードを記憶し、再生時にコンテンツの再生制約コードに応じた制約になるように記録または再生の制御を行うことを特徴とする請求項１記載のデータ管理カード。

【請求項７】異なる暗号アルゴリズムである第１暗号部と第２暗号部を有するカードを用い、前記第１暗号部で暗号されて伝送されてくる情報を復号し、情報をメディアに記録する場合は第２暗号部を用いて暗号化することを特徴とするデータ管理方法。

【請求項８】乱数を鍵として暗号化したコンテンツと乱数を用いた独特の識別コードをメディアに記録することを特徴とする請求項７記載のデータ管理方法。

2

【請求項９】カードにコンテンツのタイトル毎に識別コードと復号鍵を持たせ、コンテンツを再生する場合に前記識別コードを用いて、前記カード外部に鍵情報を公開することなく復号化することを特徴とする請求項７記載のデータ管理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、メディア記録されたコンテンツの再生に必要な情報を、カードを用いて管理するシステムに用いられるデータ管理カードに関するものである。

【０００２】

【従来の技術】有線テレビジョン放送などでは、情報発信側である放送局と受信側との間で結ばれた契約内容に応じて、契約者になったユーザに発信される。具体的にはビデオ、オーディオ等のコンテンツを発信側が著作権保護するために暗号化し、受信契約を結んだユーザにＩＣカードを発行し、契約者のみに復号化を可能にする限定受信システムが導入されている。

【０００３】この限定受信システムでは、契約者側のＩＣカードが備えられた受信装置で放送局側から暗号化されて配信されたコンテンツを復号して視聴する。

【０００４】

【発明が解決しようとする課題】しかしながら、上記従来の構成では、発信側から伝送されたコンテンツをメディアに記録する場合に、記録したいコンテンツを暗号化したままで記録し、再生時に復号することが考えられるが、発信の暗号方式が解読された場合に、メディアに暗号化して記録しているコンテンツを自由に復号化することが可能であり、著作権保護の観点で問題を有していた。

【０００５】また、コンテンツを復号するための鍵を暗号化してメディアに配置したとしても、例えばディスク系、テープ系にしろ、メディアを再生できる装置であれば記録データを容易に取得可能であり、解読の危険性と言う点で問題を有していた。

【０００６】また、著作権保護の観点から、コンテンツメーカの要望として以下（１）～（４）が求められている。

【０００７】（１）メディアに記録されたコンテンツを別の装置（メディア）に出力する場合に、その回数を制限する。

【０００８】（２）メディアに記録したコンテンツを再生する毎に料金を徴収するための再生課金。

【０００９】（３）メディアにコンテンツを記録する場合に、不正なコンテンツの流通を防止するために、コンテンツの発信源を識別可能な情報の保持。

【００１０】（４）メディアに記録されたコンテンツを別の装置（メディア）に出力する場合に、そのコンテンツの視聴の条件を制約する。

【００１１】上記要望を実行する方法としては、各制御情報をコンテンツと共にメディアに記録することで行うことが考えられるが、前記理由により適切ではなく、メディアへの記録または再生可能な装置自身に保持する方法もあるが、装置を制御するＣＰＵのプログラムへの改竄による不正行為が考えられる。

【００１２】そのため、メディアでもなく、装置でもないセキュリティ機能を有する著作権保護を行う第３者の存在が望まれる。

【００１３】本発明は、上記従来の問題点を解決するためになされたものであり、メディアへの記録または再生可能な装置にインターフェースを内蔵した取り外し可能でセキュリティ機能を付加可能なカードを用いて上記（１）～（４）および下記（５）、（６）の機能を提供することを目的とする。

【００１４】（５）インターフェースを介した通信とメディアのコンテンツに用いる暗号アルゴリズムが異なる様に機能する。

【００１５】（６）メディアに暗号化したコンテンツを記録した場合に、コンテンツを復号化する鍵をメディアに記録することなく復号可能である。

【００１６】

【課題を解決するための手段】本発明は上記目的を達成するために、第１発明に係わるデータ管理カードは、メディアへの記録または再生する装置と通信することでコンテンツの管理を行うために２種類以上の暗号アルゴリズムと、外部装置との通信を目的とするインターフェースを少なくとも有し、メディアに記録するデータに用いる暗号アルゴリズムとインターフェースで通信に用いる暗号アルゴリズムが異なる様に変換することを備えた構成を有する。

【００１７】第２発明に係わるデータ管理カードは、メディアにコンテンツを暗号化して記録する場合において、乱数を発生する乱数発生器を備え、乱数発生器を用いて記録するコンテンツ単位（名）で暗号化するための鍵を作成し、記録するデータ単位（名）毎に異なる様に乱数発生器を用いて独特の識別コードの情報を作成し、該カードとメディアに同一識別コードを記憶することを備えた構成を有する。

【００１８】第３発明に係わるデータ管理カードは、メディアに記録されているコンテンツのインターフェースから外部装置への出力を制限する複写回数制限コードの情報を記憶し、記録回数制限コードを有するコンテンツを出力する場合にコンテンツ毎に複写回数制限コードを更新し、所定値になることで外部への出力を不可能とすることを備えた構成を有する。

【００１９】第４発明に係わるデータ管理カードは、メディアに記録したコンテンツを再生する毎に料金を徴収するための再生課金に際し、コンテンツ毎に料金識別するための等級コードの情報と、日付を示す日付コードの情報と、日付コードにより等級コードを選択するための転送コードの情報を有し、ディスクへの記録時にコンテンツ毎に等級コードと前記日付コードを記憶し、再生時において等級コードより選択される料金を加算することを備えた構成を有する。

【００２０】第５発明に係わるデータ管理カードは、メディアにインターフェースを介してコンテンツを記録する場合、該コンテンツの発信源を識別可能なトレースコードの情報を記憶することを備えた構成を有する。

【００２１】第６発明に係わるデータ管理カードは、コンテンツの視聴の条件を制約する再生制約コードの情報を付加されたコンテンツをメディアに記録または再生する場合、記録時に再生制約コードを記憶し、再生時にコンテンツの再生制約コードに応じた制約になるように前記記録または再生する装置を制御することを備えた構成を有する。

【００２２】

【発明の実施の形態】以下、本発明の実施の形態について、図面を参照しながら説明する。

【００２３】（コンテンツの配信）公開のネットワークを介してコンテンツを配信するコンテンツ送受信システムについて説明する。図１はコンテンツを送受信するシステム図である。

【００２４】図１において、１００はコンテンツの配信側である放送発信局、１０１は契約により放送発信局１００からの情報を受信およびメディアへの記録または再生可能なユーザ側の受信記録再生装置、１０２は契約することで発行されるカード、１０３は公開上のネットワーク、１０４はテレビ、１０５はカード１０２から他の装置へのデータの送受信を行うためのインターフェースの通信ケーブルである。

【００２５】放送発信局１００から発信されるコンテンツとしては、映画などのビデオ、ジャズなどのオーディオ、ゲーム、著作物などの文字情報等であり、伝送コンテンツは暗号化されている。

【００２６】本実施の形態では、コンテンツはＭＰＥＧ２（ＩＳＯ　１３８１８－２）の伝送フォーマットであるトランスポートストリームを用いて伝送するビデオとして説明する。

【００２７】このコンテンツ送受信は、放送発信局１００からコンテンツを暗号化してネットワーク１０３を介してユーザの受信記録再生装置１０１に伝送され、受信記録再生装置１０１で復号することでテレビ１０４に再生する。

【００２８】コンテンツを暗号化する方式としては、同じ鍵データを有する共通鍵暗号方式とし、この場合、ユーザが受信契約することで発行されたカード１０２と放送発信局１００に共通鍵（マスタ鍵）を有することにより、図２のように行うものとする。

【００２９】まず、送信側では、配信するコンテンツを

暗号化するためのコンテンツ鍵１０８を生成し、コンテンツ鍵１０８を用いて暗号部１０７によりコンテンツを暗号化したコンテンツ情報とコンテンツ鍵１０８をマスタ鍵１０９を用いて暗号部１０７により暗号化したコンテンツ鍵情報を受信側にネットワーク１０６を介して伝送する。

【００３０】受信側では、暗号化したコンテンツ鍵情報を、マスタ鍵１１１を用いて復号部１１０により復号化してコンテンツ鍵１１２とし、暗号化したコンテンツ情報を、コンテンツ鍵１１２を用いて復号化することでコンテンツが暗号化伝送される。

【００３１】伝送されるコンテンツはタイトル毎に所定の単位で分割して図３に示す様に行われるものとする。図３はコンテンツを伝送するフォーマットを示す図である。

【００３２】図３において、１１３はフォーマットの先頭を示すプリアンブル、１１４はコンテンツの送信先を示す送信先アドレス、１１５はコンテンツの送信元を示す送信元アドレス、１１６は送信データであるデータ部であり、１１７はタイトル等のデータを配置したヘッダ情報部、１１８はコンテンツを復号するためのコンテンツ鍵である復号鍵情報部、１１９はコンテンツ情報から構成されたコンテンツ情報部である。ここで、ヘッダ情報部１１７はタイトル単位で同一情報とする。

【００３３】（コンテンツのメディアへの記録）放送発信局１００からのコンテンツを受信記録再生装置１０１への記録動作について説明する。図４はカード１０２における構成図である。

【００３４】図４において、２００は受信記録再生装置１０１とデータの送受信を行うためのカードＩ／Ｏ、２０１はカード１０２を制御するＣＰＵ、２０２はＣＰＵ２０１が実行するプログラムを記憶しているＲＯＭ、２０３は放送発信局１００から配信されるコンテンツに用いられる暗号アルゴリズムを備えた暗号部α、２０４は乱数を発生する乱数発生器、２０５は受信記録再生装置１０１の外部装置とデータの送受信を行うインターフェース、２０６は配信されたコンテンツをメディア等に記＊録する場合に用いられる暗号アルゴリズムを備えた暗号部β、２０７は放送発信局から配信された暗号化したコンテンツを復号するための鍵であるマスタ鍵、２０８はコンテンツの再生に必要な情報を記憶する不揮発性メモリで構成された管理情報部、２０９は後述する再生課金の処理に用いられる不揮発性メモリで構成された再生課金テーブル部である。

【００３５】図５は受信記録再生装置１０１における構成図であり、図５において、２１０は公開上のネットワーク１０３を介して放送発信局１００とデータの送受信を行うためのネットワークインターフェース、２１１はＭＰＥＧのビデオ、オーディオのデータを復号する伸長処理部、２１２はカード１０２とデータの送受信を行うためのカードＩ／Ｏ、２１３は記録フォーマットを作成する信号処理部、２１４はレーザ駆動部、２１５は光ヘッド部、２１６はディスク、２１７は受信記録再生装置１０１を制御するＣＰＵ２１８はユーザが受信記録再生装置１０１の動作を設定する設定部２１８である。

【００３６】ここで、カード１０２はカードＩ／Ｏ２００と受信記録再生装置１０１のカードＩ／Ｏ２１１で通信できる様に受信装置１０１に配置する。

【００３７】表１は管理情報部２０８における記憶データのフォーマットで、３００はコンテンツのタイトル、３０１はコンテンツ毎の識別を行う識別コード、３０２はコンテンツを暗号化して記録する場合における鍵、３０３はコンテンツを外部に出力する場合にその回数を制限する複写回数制限コード、３０４はコンテンツ毎のメディアに記録した時における再生課金するための料金を識別する等級コード、３０５はコンテンツ毎の記録した時における日付を示す日付コード、３０６はメディアに記録したコンテンツの再生装置外部への出力における品位を制約する再生制約コード、３０７はコンテンツを記録する場合にコンテンツ毎の配信源を記録するトレースコード、３０８は再生課金した場合の課金料金である。

【００３８】

【表１】

300	301	302	303	304	305	306	307	308
				再生課金部				
タイトル	識別コード	鍵	複写回数制限コード	等級コード	日付コード	再生制約コード	トレースコード	課金料金
X ・ ・	B ・ ・	A ・ ・	2 ・ ・	T1	1999. 4	011		

【００３９】タイトルＸのコンテンツを受信記録再生装置１０１へ記録する動作について説明する。まず、放送発信局１００からネットワーク１０３を介して暗号化した形式で伝送したコンテンツは、受信記録再生装置１０１のネットワークインターフェース２１０で受信し、カードＩ／Ｏ２１２よりカード１０２に伝送する。

【００４０】カード１０２ではＲＯＭ２０２の制御プログラムをＣＰＵ２０１が実行することで図６に示す様にステップＳ１１では乱数部２０４において第１の乱数を発生し鍵Ａとし、ステップＳ１２では乱数部２０４にお

いて第２の乱数を発生し乱数Ａとし、ステップＳ１３では乱数Ａと管理情報部２０８に識別コードとして登録されている情報を比較し、一致した場合（ｎｏ）はステップＳ１２を実行し、不一致した場合（ｙｅｓ）はステップＳ１４において乱数Ａを識別コードＢとする。これにより後述する記録時にコンテンツを暗号化するための鍵と再生時にそのコンテンツの復号に必要なカード１０２に記憶した鍵を識別可能とする識別コードのペアを作成する。

【００４１】そして、カードＩ／Ｏ２００を介して入力したコンテンツを所定の単位でマスタ鍵２０７を用いて暗号部α２０３により復号化し、そのコンテンツを、鍵Ａを用いて暗号部β２０６により暗号化し、識別コードＢと暗号化したコンテンツをカードＩ／Ｏ２００から受信記録再生装置１０１に送信し、かつ鍵Ａと識別コードＢと詳細は後述するが、ヘッダ情報部１１７に含まれる情報を管理情報部２０８にタイトル単位で表１の様に記憶する。ここで、設定がなければ０として以降説明する。

【００４２】受信記録再生装置１０１はカードＩ／Ｏ２１２で受信した識別コードとコンテンツを信号処理部２１３においてエラーを訂正するためのエラー訂正コードを付加し記録フォーマットに変換し、その記録情報をレーザ駆動部２１４において電気信号を光学信号に変換するめの処理を行い、光ヘッド部２１５によりディスク２１６に記録する。

【００４３】以上の動作によりネットワークを介したコンテンツの配信に用いる暗号アルゴリズムとメディアへの記録または再生可能な装置に用いる暗号アルゴリズムを異なる様にすることで、ネットワークに用いる暗号アルゴリズムが解読されてもメディアに暗号化して記録しているコンテンツの復号は不可能であり、コンテンツに著作権保護の安全性が強固となる。

【００４４】また、カード内でコンテンツの暗号を変換することで、変換過程の平文を外部に公開することなくコンテンツのセキュリティが保たれたまま暗号の変換ができる。

【００４５】（メディアからのコンテンツ再生）受信記録再生装置１０１に記録しているタイトルＸのコンテンツの再生について説明する。まず、受信記録再生装置１０１はディスク２１６からタイトルＸのコンテンツと識別コードＢを光ヘッド部２１５より光学的に読み出した情報をレーザ駆動部２１４において電気信号に変換し、信号処理部２１３においてエラー訂正を行い、カードＩ／Ｏ２１２より識別コードＢとコンテンツをカード１０２に送信する。

【００４６】カード１０２ではＲＯＭ２０２の制御プログラムをＣＰＵ２０１が実行することでカードＩ／Ｏ２００よりコンテンツと識別コードＢを入力し、識別コードＢを管理情報部２０８に記録されている識別コードと比較し、一致した場合には一致した識別コードにおける鍵（Ａ）を用いて暗号部β２０６によりコンテンツを復号化してカードＩ／Ｏ２００より受信記録再生装置１０１に送信する。

【００４７】受信記録再生装置１０１ではカードＩ／Ｏ２１２より受信したコンテンツを伸長処理部２１１でＭＰＥＧ処理を行い、ビデオまたはオーディオを出力する。

【００４８】以上の動作により暗号化してコンテンツをメディアに記録した場合に、コンテンツに鍵情報をメディアに記録せず独特な（識別コード）コードを記録し、識別して再生可能にすることで、鍵をカード外部に公開することなく復号可能となり、著作権を強固にすることができる。

【００４９】以降再生動作におけるカード１０２の動作について説明する。

【００５０】（他のメディアへのデジタル出力の回数制限）受信記録再生装置１０１のディスク２１６から再生したコンテンツを、図７にある様にカード１０２のインターフェース２０５から通信ケーブル１０５を介して接続した外部装置である記録装置１０６へのコンテンツのデジタル出力の制限について説明する。

【００５１】ここで、前記表１の複写回数制限コードは、データを設定しない場合は０とし、設定した場合においてデジタル出力するごとにカウントダウンして１となった場合にデジタル出力不許可とするものとし、例えば１回だけディジタル出力を許可する場合は２を設定するものとし、受信記録再生装置１０１の設定部２１８より外部装置である記録装置１０６へのコピー動作を設定した場合におけるカード１０２の動作を説明する。

【００５２】ステップＳ２１では複写回数制限コードと０を比較し、一致した場合（ｎｏ）はステップＳ２４を実行し、不一致の場合（ｙｅｓ）はステップＳ２２において複写回数制限コードと１を比較し、一致した場合（ｎｏ）はインターフェース２０５からコンテンツの出力を行わずに終了し、不一致の場合（ｙｅｓ）はステップＳ２３において複写回数制限コード－１を行い、ステップＳ２４においてインターフェース２０５からコンテンツを出力する。

【００５３】例えばタイトルＸでは、複写回数制限コードが２であることから１度だけ外部への出力が可能である。

【００５４】以上の様に、カード内部でインターフェースとインターフェースから外部へのコンテンツのコピー等の出力回数を制限できる情報をタイトル毎に備えることで、カード外部に情報が漏れることなく容易にインターフェースからのコンテンツ情報の出力を止めることができるため記録したコンテンツの著作権保護が強固となる。

【００５５】（再生課金）メディアに記録したコンテン

ツを再生する毎に料金を徴収するための再生課金について説明する。

【００５６】表２は再生課金テーブル部２０９における＊記憶データのフォーマットである。

【００５７】

【表２】

400 等級部	401 日付部	402 転送部	403 料金部	
T1	1999. 6	T10	$10	404 メインテーブル領域
T2	1999. 6	T11	$8	
T3	1999. 6	T15	$6	
：	：	：	：	
T10	1999. 5	T3	$9	405 転送テーブル領域
T11	1999. 4	T15	$7	
：	：	：	：	

【００５８】表２において、４００はコンテンツの料金を識別するためのコードである等級部、４０１は等級部４００の各情報の日付を示す日付部、４０２は料金検索における番地を示す転送部、４０３は再生課金の料金を示す料金部、４０４は再生課金における基本料金を示すメインテーブル領域、４０５は基本料金以外の料金を示す転送テーブル領域である。

【００５９】ここで、日付コード３０５および日付部４０１における日付情報は（西暦．月）で表示するものと、再生課金の料金を確定する際、転送部４０２が示す等級部４００のコードが転送テーブル領域４０５からメインテーブル領域４０４へ検索動作が移動した場合には、その等級部４００のコードにおける料金部４０３の料金を無条件に課金するものとする。

【００６０】ステップＳ３１では、再生するコンテンツの等級コード３０４をメインテーブル４０４における等級部４００のコードと比較し、不一致の場合（ｎｏ）は再生を終了し、一致した場合（ｙｅｓ）は一致したコードの情報を参照し、ステップＳ３２を実行する。

【００６１】ステップＳ３２において、一致した等級部４００のコードにおける日付部４０１とコンテンツの日付コード３０５の日付情報を比較し、日付コード３０５≧日付部４０１の場合（ｙｅｓ）は、ステップＳ３５において料金確定として料金部４０３における該コンテンツの料金を課金料金３０８に加算し、日付コード３０５＜日付部４０１つまり日付コード３０５が古い場合（ｎｏ）は、ステップＳ３３において該等級部４００のコードにおける転送部４０２が示す転送テーブル領域４０４における等級部４００のコードにおける日付部４０１と該コンテンツの日付コード３０５を比較する。

【００６２】ステップ３３において、日付コード３０５≧日付部４０１の場合（ｙｅｓ）はステップＳ３５において料金確定として料金部４０３における該コンテンツの料金を課金料金３０８に加算し、日付コード３０５＜日付部４０１つまり日付コード３０５が古い場合（ｎｏ）はステップＳ３４を実行する。

【００６３】ステップＳ３４において、該転送部４０２におけるコードとメインテーブル領域４０４の最終コード（Ｔ９）とを比較し、メインテーブル領域４０４以内のコードであれば、ステップＳ３５において、料金確定として料金部４０３における該コンテンツの料金を課金料金３０８に加算し、以外のコードであれば、転送テーブル領域４０５においてステップＳ３３を実行する。

【００６４】例えば、タイトルＸを再生する場合は、ステップＳ３１において等級コード３０４がＴ１なので等級部４００のＴ１における情報を参照し、ステップＳ３２においてタイトルＸの日付コード３０５と等級部４００のＴ１における日付部４０１の日付情報を比較し、日付コード３０５が古いことから、ステップＳ３３において転送部４０２が示す転送テーブル領域４０５における等級部４００のＴ１０の日付部４０１とタイトルＸの日付コード３０５における日付情報を比較し、日付コード３０５が古いことからステップＳ３４において転送部４０２が示す等級部３００のコードがメインテーブル領域４０４を示すかを確認し、転送部４０２はＴ３であることからメインテーブル領域４０４なので、ステップＳ３５において等級部４００のＴ３における料金部４０３を課金料金３０８に加算し、タイトルＸの再生課金を行う。

【００６５】そして、定期的に受信記録再生装置が課金料金３０８を放送発信局１００に送信することで、後で放送発信局１００は課金料金３０８を基に銀行口座等から課金料金を引き落とす。

【００６６】メディアにコンテンツを記録した場合における料金のランクを示す等級コードと日付けを示す日付コードをカードに記憶しておき、放送発信局１００から定期的に配信される課金データブル情報を再生課金テーブル部２０９に有する様にし、再生する際に上記動作をすることによりコンテンツの再生課金を行うことで、コンテンツは時が進むにつれ社会的価値（時価）が変わることから、メディアに記録したコンテンツを再生した時の時価で再生課金することができる。

【００６７】（再生制約の動作）メディアに記録したコンテンツを別の装置（メディア）に出力する場合に、そのコンテンツの視聴条件の制約について説明する。

【００６８】表３はコンテンツの制約情報であり、この＊情報の内容をＲＯＭ２０２に有するものとする。

【００６９】

【表３】

コード	制約
<ビデオ>	
001	SDをサブサンプリング（間引き）する。
010	プログレッシブ（ノンインターレス）をインターレスかする。
011	HDをSD以下にダウンコンバートする。
<オーディオ>	
101	ダウンサンプリングする。（48kHz系→16kHz、44.1kHz系→13.7kHz）
110	チャンネル（ch）制限する。（2chの有効（5.1ch→2ch））
111	上記101、110を共に行う。

【００７０】ステップＳ４１では再生するコンテンツの再生制約コード３０６と０を比較し、一致した場合（ｎｏ）は再生するコンテンツへの制約は無しとし、不一致の場合（ｙｅｓ）は制約情報が有るものとしてステップＳ４２において再生制約コード３０６に応じてＲＯＭ２０２に有る制約情報の内容を実行する。

【００７１】例えば、タイトルＸであれば、再生制約コード３０６が０１１なので、ＣＰＵ２０１において高細精なハイビジョン（ＨＤ）のビデオデータの走査線数を現行テレビ放送（ＮＴＳＣ）レベルまで操作（減少）してから、インターフェース２０５から通信ケーブル１０５を介して出力する。

【００７２】メディアに記録したコンテンツの再生制約の条件を示す再生制約コードをカードに記憶しておき、外部の装置にインターフェースを介してコンテンツを出力する際に上記動作をすることで、仮にコピーしたとしてもオリジナルとの品質における差別化が可能であり、オリジナルの価値の低下を防ぐことができる。

【００７３】（トレース動作）メディアに記録したコンテンツの発信源の送信元アドレス１１５をカードに記録しておくことで、ネットワーク１０３を介して不正コピーされたコンテンツを記録した場合にその発信源が特定できる。

【００７４】

【発明の効果】以上のように本発明によれば、下記の特徴を備えたカードを用いることで、メディア等に記憶したコンテンツの著作権保護が強固となる。

【００７５】（１）ネットワークを介したコンテンツの配信に用いる暗号アルゴリズムとメディアへの記録または再生可能な装置に用いる暗号アルゴリズムを異なるようにすることで、ネットワークに用いる暗号アルゴリズムが解読されても、メディアに暗号化して記録しているコンテンツの復号は不可能であり、コンテンツに著作権保護の安全性が強固となる。

【００７６】また、カード内でコンテンツの暗号を変換することで、変換過程の平文を外部に公開することなく、コンテンツのセキュリティが保たれたまま暗号の変換ができる。

【００７７】（２）コンテンツは時が進むにつれ社会的価値（時価）が変わるため、メディアに記録したコンテンツを再生した時の時価で再生課金することができる。

【００７８】（３）暗号化してコンテンツをメディアに記録する場合に、コンテンツに鍵情報をメディアに記録せず、独特なコードを記録し識別して再生可能にすることで、鍵をカード外部に公開することなく復号可能となり、著作権を強固にすることができる。

【００７９】（４）カードにインターフェースとコンテンツ毎の出力回数を制限する情報を保持することで、カード自身が不正コピーの検出し、阻止することができる。

【００８０】（５）ネットワークを介してコンテンツを記録する場合に、そのコンテンツの発信源であるアドレスを保持することで、不正コピーが流通した場合に、その発信源が特定できる。

【００８１】（６）デジタル出力するコンテンツの視聴条件を制約する情報を保持し、制約情報に応じてデジタル出力するコンテンツの品質を制約することで、仮にコピーしたとしても、オリジナルとの品質における差別化が可能であり、オリジナルの価値の低下を防ぐことができる。

【図面の簡単な説明】

【図１】本発明の一実施例における伝送システムの構成図

【図２】同伝送システムにおけるコンテンツの暗号化伝送構成を示すブロック図

【図３】同伝送システムの伝送フォーマット構成図

【図４】同伝送システムに用いられるカードの構成図

【図５】同伝送システムの受信記録再生装置の構成図

【図６】同識別コード生成におけるフローチャート

【図７】本実施例における他の伝送システムの構成図

【図８】本実施例の記録コンテンツの出力の制限におけるフローチャート

【図９】本実施例の再生課金におけるフローチャート

【図１０】本実施例の記録コンテンツの出力における制約を検出するフローチャート

【符号の説明】

１００　放送発信局

１０１　受信記録再生装置

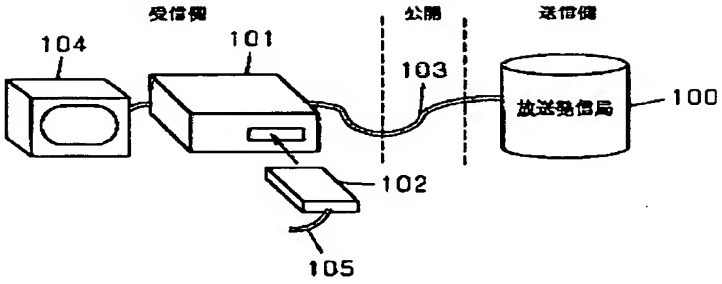
13

１０２　カード
１０３　ネットワーク
１０４　テレビ
１０５　通信ケーブル
１０６　記録装置
２００　カードＩ／Ｏ
２０１　ＣＰＵ
２０２　ＲＯＭ
２０３　暗号部α
２０４　乱数部
２０５　インターフェース
２０６　暗号部β
２０７　マスタ鍵
２０８　管理情報部
２０９　再生課金テーブル部
２１０　ネットワークインターフェース
２１１　伸長処理部
２１２　カードＩ／Ｏ
２１３　信号処理部
２１４　レーザ駆動部

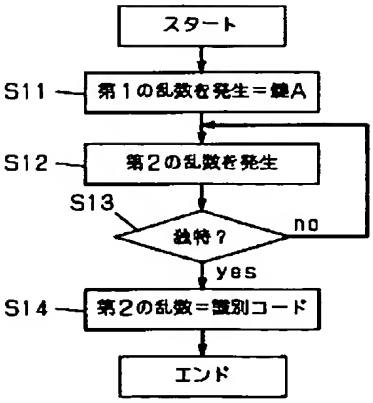
14

＊２１５　光ヘッド部
２１６　ディスク
２１７　ＣＰＵ
２１８　設定部
３００　タイトル
３０１　識別コード
３０２　鍵
３０３　複写回数制限コード
３０４　等級コード
３０５　日付コード
３０６　再生制約コード
３０７　トレースコード
３０８　課金料金
４００　等級部
４０１　日付部
４０２　転送部
４０３　料金部
４０４　メインテーブル領域
４０５　転送テーブル領域

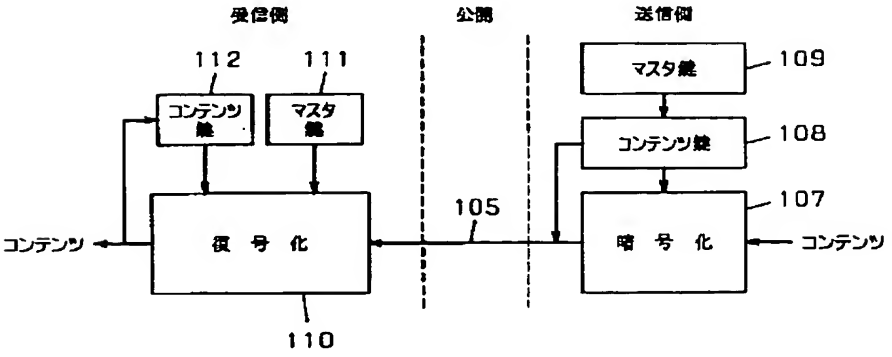
【図１】



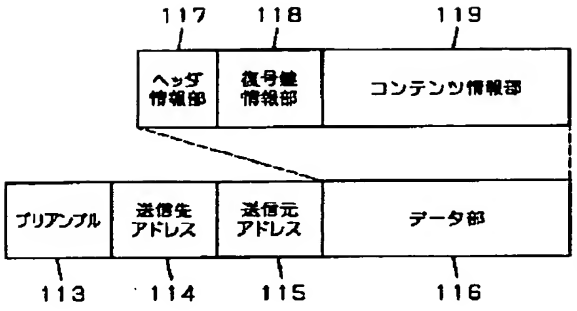
【図６】



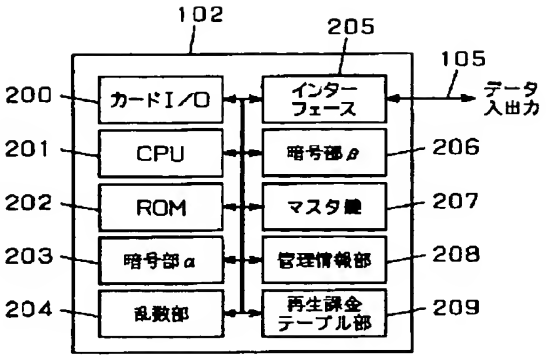
【図２】



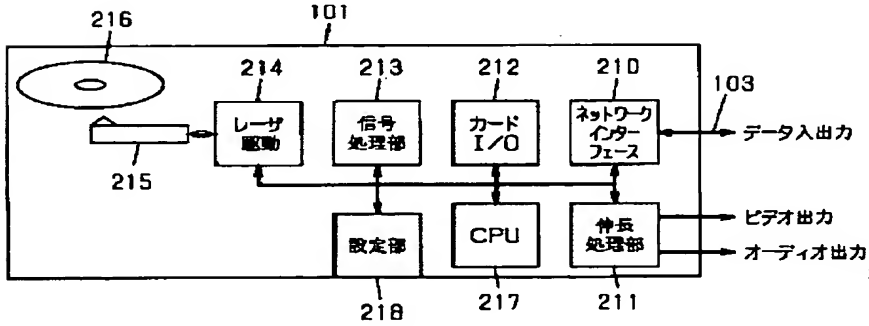
【図３】


117
118
119
ヘッダ情報部
復号鍵情報部
コンテンツ情報部
プリアンブル
送信先アドレス
送信元アドレス
データ部
113
114
115
116

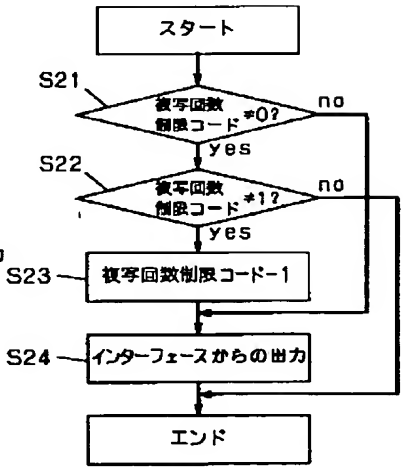
【図４】


102
205
105
200
201
202
203
204
カードI/O
CPU
ROM
暗号部α
乱数部
インターフェース
暗号部β
マスタ鍵
管理情報部
再生課金テーブル部
データ入出力
206
207
208
209

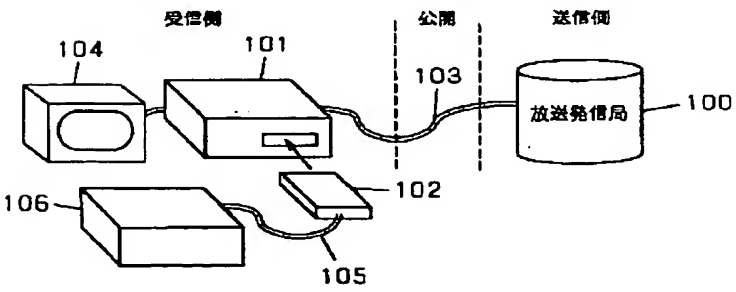
【図５】


216
101
214
213
212
210
103
215
レーザ駆動
信号処理部
カードI/O
ネットワークインターフェース
データ入出力
設定部
CPU
伸長処理部
ビデオ出力
オーディオ出力
218
217
211

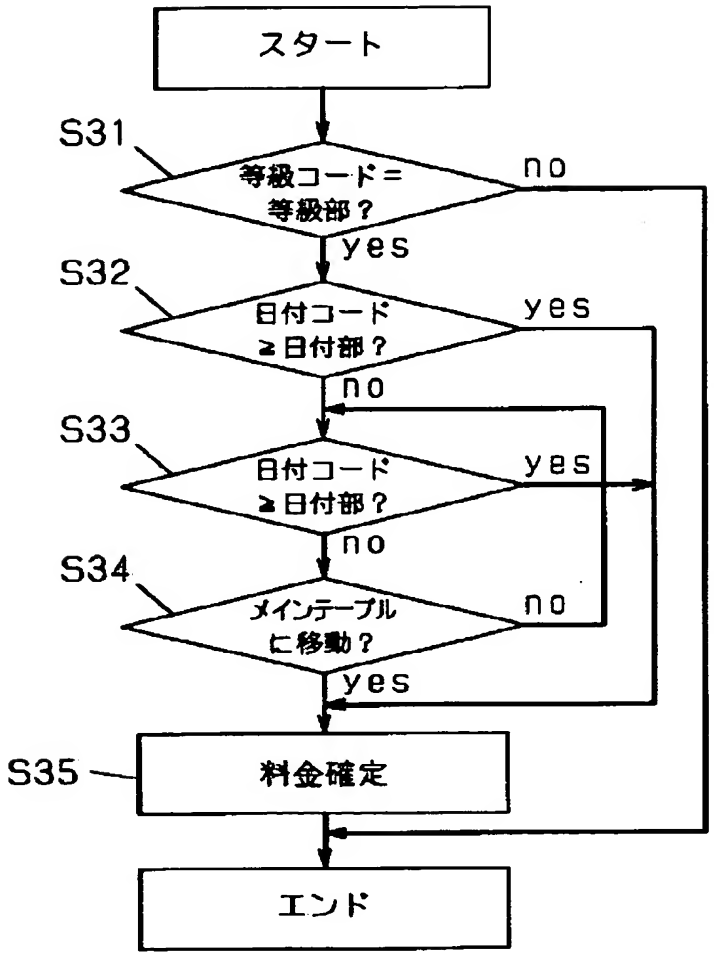
【図８】


スタート
S21
複写回数制限コード≠0?
no
yes
S22
複写回数制限コード≠1?
no
yes
S23
複写回数制限コード-1
S24
インターフェースからの出力
エンド

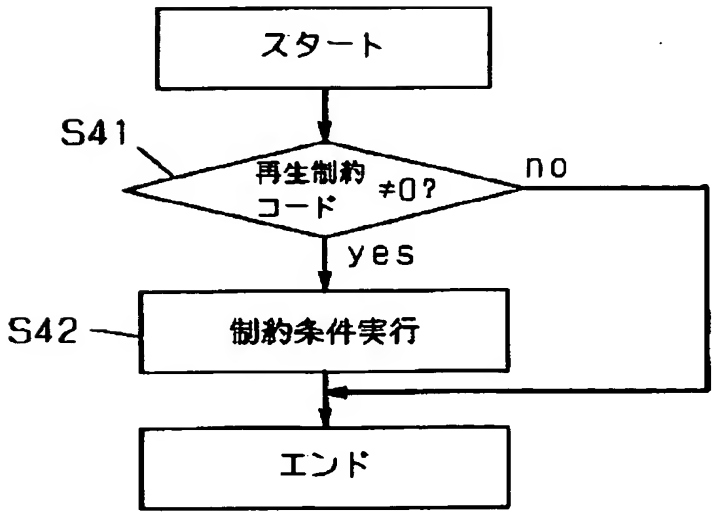
【図７】


受信側
公開
送信側
104
101
103
放送発信局
100
102
106
105

【図９】


スタート
S31
等級コード＝
等級部？
no
yes
S32
日付コード
≧日付部？
yes
no
S33
日付コード
≧日付部？
yes
no
S34
メインテーブル
に移動？
no
yes
S35
料金確定
エンド

【図１０】


スタート
S41
再生制約
コード
≠0？
no
yes
S42
制約条件実行
エンド

フロントページの続き

Ｆターム(参考) 5B035 BB09 BC00 CA08 CA11
5B085 AE12 AE29
5C064 CA14 CB08 CC04
5J104 AA01 AA07 AA12 AA16 AA34
AA41 EA04 EA08 EA16 EA22
JA03 KA01 KA02 NA02 NA35
NA36 NA37 NA40 PA06 PA11